Imagen que contiene texto, libro

Descripción generada automáticamente

|  |
| --- |
|  |
| **DIRECCIÓN GENERAL DE TECNOLOGÍAS DE INFORMACIÓN E INNOVACIÓN** |
| **DIRECCIÓN DE SEGURIDAD TECNOLÓGICA** |
| **INFORME DE ANÁLISIS DINÁMICO**  **“cursosenlinea.sre.gob.mx– Análisis dinámico”**  SE-21-014  08|2021 |
|  |

Contenido

[I. Introducción 3](#_Toc80706193)

[II. Antecedentes 3](#_Toc80706194)

[III. Resumen Ejecutivo 3](#_Toc80706195)

[IV. Vulnerabilidades identificadas 3](#_Toc80706196)

[V. Plan de acción 4](#_Toc80706197)

[A. Objetivo general 4](#_Toc80706198)

[B. Metodología 4](#_Toc80706199)

[VI. Alcance de la evaluación 6](#_Toc80706200)

[VII. Estructura del Reporte 7](#_Toc80706201)

[A. Página de inicio de sesión susceptible a ataques de fuerza bruta 7](#_Toc80706202)

[B. HSTS falta en el servidor HTTPS 9](#_Toc80706203)

[C. Uso de componentes vulnerables u obsoletos 11](#_Toc80706204)

[D. Métodos HTTP TRACE / TRACK permitidos 13](#_Toc80706205)

[E. Aplicación web potencialmente vulnerable al secuestro de clics 15](#_Toc80706206)

[VIII. Descripción de la criticidad 17](#_Toc80706207)

[IX. Resumen técnico de hallazgos 18](#_Toc80706208)

[X. Recomendaciones 18](#_Toc80706209)

[XI. Firmas y fechas de elaboración, revisión, recepción y aprobación 19](#_Toc80706210)

# Introducción

El equipo de seguridad informática de TIC DEFENSE por parte del equipo de pruebas de penetración, realiza el análisis dinámico con el objetivo de identificar vulnerabilidades que afecten la integridad, confidencialidad y disponibilidad de los sistemas e información involucrados.

# Antecedentes

De acuerdo con la solicitud realizada por la Secretaría, se realiza el análisis de vulnerabilidades Al siguiente componente:

* **https://cursosenlinea.sre.gob.mx/**

El equipo de seguridad de TIC DEFENSE procedió a realizar el análisis dinámico.

# Resumen Ejecutivo

Con el propósito de identificar las vulnerabilidades potenciales que pudieran comprometer la seguridad de la Información, se realizó el este análisis dinámico del aplicativo. Las vulnerabilidades identificadas podrían permitir a un usuario malintencionado realizar ataques de fuerza bruta para para hallar credenciales válidas y usar vulnerabilidades conocidas de componentes obsoletos. Estos se clasifican con un riesgo **ALTO**, por lo que se considera que se deben realizar acciones inmediatas para mitigar las vulnerabilidades expuestas ya que estas podrían afectar directamente a la confidencialidad e integridad de los sistemas involucrados.

# Vulnerabilidades identificadas

A continuación, se muestra una gráfica de las vulnerabilidades identificadas durante las pruebas de penetración realizadas a **cursosenlinea.sre.gob.mx.**

|  |  |
| --- | --- |
| **CRITICIDAD** | **VULNERABILIDADES IDENTIFICADAS** |
|  |
| ALTA | 1. Página de inicio de sesión susceptible a ataques de fuerza bruta |  |
| MEDIA | 2. HSTS falta en el servidor HTTPS |  |
| MEDIA | 3. Uso de componentes vulnerables u obsoletos |  |
| INFORMATIVA | 4. Métodos HTTP TRACE / TRACK permitidos |  |
| INFORMATIVA | 5. Aplicación web potencialmente vulnerable al secuestro de clics |  |

***Nota: La criticidad de las vulnerabilidades mencionadas en este documento, se cataloga de acuerdo con el escenario evaluado, por lo tanto, esta puede variar respecto al criterio de la secretaría (SRE) al igual que el nivel de prioridad para su remediación.***

# Plan de acción

## Objetivo general

Presentar los resultados de las pruebas realizadas a **cursosenlinea.sre.gob.mx,** con la finalidad de identificar vulnerabilidades críticas dentro de los sistemas involucrados.

## Metodología

Las pruebas de seguridad están basadas en la metodología OWASP para evaluar la seguridad de un sistema, un aplicativo o red, validando y verificando metódicamente la efectividad de controles de seguridad de aplicaciones, realizándose una prueba de seguridad de aplicaciones web que se centra en evaluar la seguridad de la aplicación web, en el cual los procesos que se implican en un análisis activo son por cualquier debilidad, fallas técnicas o vulnerabilidades.

La prueba se divide en 2 fases:

* Modo pasivo:

En el modo pasivo, se intenta comprender la aplicación lógicamente, manipulando la aplicación para recopilar información comprendiendo la configuración implementada del servidor que aloja la aplicación web. Siendo en las plataformas de aplicación amplias y variadas, puede haber algunas claves o señales en errores de configuración que comprometen la aplicación, de la misma manera que una aplicación no segura puede comprometer el servidor. Por ejemplo, se puede usar un web proxy para observar todas las solicitudes y respuestas HTTP. Al final, se debe comprender todos los puntos de acceso de la aplicación (por ejemplo, encabezados HTTP, parámetros, recursos, archivos de configuración, complementos, cookies).

* Modo activo:

En esta fase, se comienza a probar utilizando la metodología descrita en la siguiente lista.

El conjunto de pruebas activas se ha dividido en subcategorías y controles:

* Recopilación de información
* Pruebas de configuración y gestión de implementación
* Pruebas de gestión de identidad
* Pruebas de autenticación
* Pruebas de autorización
* Pruebas de gestión de sesiones
* Prueba de validación de entrada
* Manejo de errores
* Criptografía
* Pruebas de lógica empresarial
* Pruebas del lado del cliente

Cualquier problema de seguridad que sea encontrado será presentado al equipo de desarrollo o infraestructura, junto con una evaluación de la criticidad, con una propuesta de mitigación o una solución técnica.

# Alcance de la evaluación

|  |  |
| --- | --- |
| **Dirección IP** | 74.208.218.19 |
| **URL** | [https://cursosenlinea.sre.gob.mx](https://spcqa.sre.gob.mx) |
| **Descripción** | Sistema cursosenlinea.sre.gob.mx |
| **Sistema Operativo** | Linux |

# Estructura del Reporte

A continuación, se presenta la estructura del documento para los hallazgos identificados

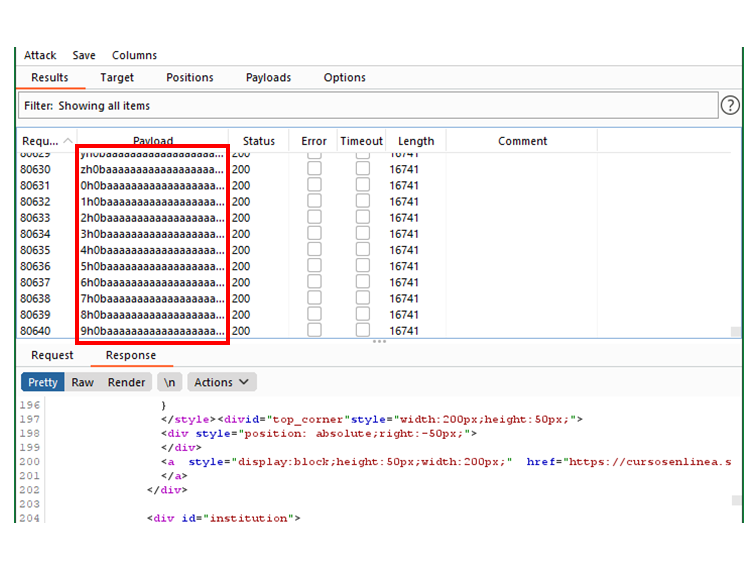
## Página de inicio de sesión susceptible a ataques de fuerza bruta

| **CWE-307** | PÁGINA DE INICIO DE SESIÓN SUSCEPTIBLE A ATAQUES DE FUERZA BRUTA | **7.6** |
| --- | --- | --- |
| VALORACIÓNCVSS FINAL:  AV:A/AC:L/PR:N/UI:N/S:U/C:H/I:L/A:L | | |
| NÚMERO DE OCURRENCIAS  1 | | |
| CLASIFICACIÓN  Confidencialidad, Integridad y Disponibilidad | | |
| Dirección IP:  74.208.218.19 | Puerto TCP/UDP: 443 | |
| RIESGO | Un atacante podría obtener de credenciales válidas para acceder al aplicativo. | |
| DESCRIPCIÓN | El proceso denominado fuerza bruta, consiste en adivinar usuarios y contraseñas válidos por medio combinaciones de estos. La aplicación no cuenta con mecanismos de protección ante este tipo de ataques. | |
| PROPUESTA DE REMEDIACIÓN | Se recomienda habilitar mecanismos de protección ante cierto número de intentos fallidos, por ejemplo 5 intentos consecutivos. Considere un periodo de espera para que los usuarios puedan volver a autenticarse después de los intentos fallidos. | |
| REFERENCIAS EXTERNAS | https://cwe.mitre.org/data/definitions/307.html  https://owasp.org/www-community/controls/Blocking\_Brute\_Force\_Attacks | |

La vulnerabilidad se presenta en la siguiente ruta:

* https://cursosenlinea.sre.gob.mx/index.php

A continuación, se presenta la evidencia de la vulnerabilidad detectada.



En la imagen se muestran una prueba de ataque de fuerza bruta, sin completar, pero para el cuál no hay ningún mecanismo de bloqueo o protección.

## HSTS falta en el servidor HTTPS

| **CWE-523** | HSTS FALTA EN EL SERVIDOR HTTPS | **6.5** |
| --- | --- | --- |
| VALORACIÓNCVSS FINAL:  AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:N | | |
| NÚMERO DE OCURRENCIAS  1 | | |
| CLASIFICACIÓN  Integridad, confidencialidad | | |
| Dirección IP:  74.208.218.19 | Puerto TCP/UDP: 443 | |
| RIESGO | Un atacante podría realizar ataques de degradación, ataques de tipo “Man in the middle” que eliminan SSL y debilita las protecciones de secuestro de cookies. | |
| DESCRIPCIÓN | La aplicación no está aplicando HSTS, como se define en RFC 6797. HSTS es un encabezado de respuesta opcional que se puede configurar en el servidor para indicar al explorador que solo se comunique a través de HTTPS. | |
| PROPUESTA DE REMEDIACIÓN | Se recomienda configurar el servidor web remoto para utilizar HSTS. | |
| REFERENCIAS EXTERNAS | https://tools.ietf.org/html/rfc6797 | |

La vulnerabilidad se presenta en la siguiente ruta:

* https://cursosenlinea.sre.gob.mx/

A continuación, se presenta la evidencia de la vulnerabilidad detectada.



En la imagen se muestra como es posible acceder a la información del sitio sin emplear HTTPS.

## Uso de componentes vulnerables u obsoletos

| **CWE-937** | USO DE COMPONENTES VULNERABLES U OBSOLETOS | **5.3** |
| --- | --- | --- |
| VALORACIÓNCVSS FINAL:  AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N | | |
| NÚMERO DE OCURRENCIAS  1 | | |
| CLASIFICACIÓN  Confidencialidad | | |
| Dirección IP:  74.208.218.19 | Puerto TCP/UDP: 443 | |
| RIESGO | Un atacante podría explotar las vulnerabilidades conocidas del componente utilizado en la aplicación. | |
| DESCRIPCIÓN | La aplicación utiliza componentes con vulnerabilidades conocidas. | |
| PROPUESTA DE REMEDIACIÓN | Instalar los parches de seguridad correspondientes o actualizar a la última versión del componente. | |
| REFERENCIAS EXTERNAS | https://cwe.mitre.org/data/definitions/937.html  https://owasp.org/www-project-top-ten/OWASP\_Top\_Ten\_2017/Top\_10-2017\_A9-Using\_Components\_with\_Known\_Vulnerabilities | |

La vulnerabilidad se presenta en la siguiente ruta:

* https://cursosenlinea.sre.gob.mx/main/inc/lib/javascript/jquery-ui/js/jquery-ui-1.8.1.custom.min.js
* https://cursosenlinea.sre.gob.mx/main/inc/lib/javascript/jquery-1.5.1.min.js
* https://cursosenlinea.sre.gob.mx/main/inc/lib/javascript/jquery-1.4.2.min.js

A continuación, se presenta la evidencia de la vulnerabilidad detectada.



En la imagen se muestra indicios de versiones de librerías que tienen vulnerabilidades conocidas públicamente, solo hay que corroborar que se pueda actualizar a la versión más reciente.

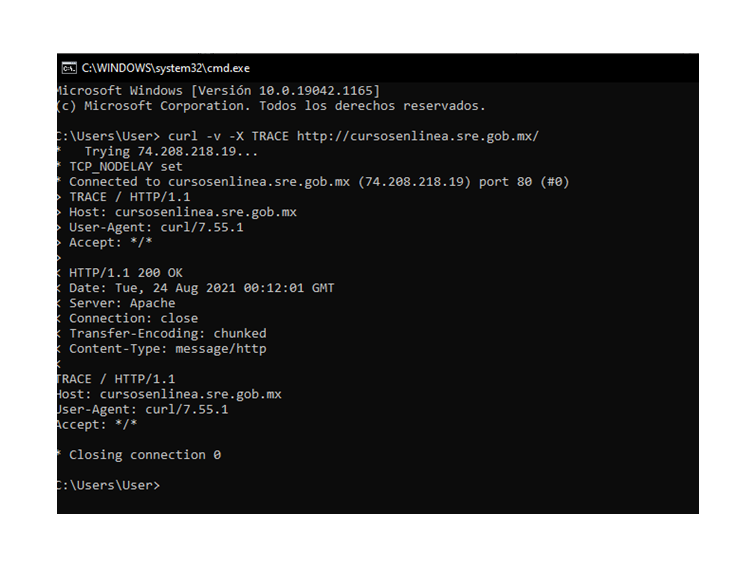
## Métodos HTTP TRACE / TRACK permitidos

| **CWE-200** | MÉTODOS HTTP TRACE / TRACK PERMITIDOS | **-** |
| --- | --- | --- |
| VALORACIÓNCVSS FINAL:  AV:A/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:N | | |
| NÚMERO DE OCURRENCIAS  1 | | |
| CLASIFICACIÓN  - | | |
| Dirección IP:  74.208.218.19 | Puerto TCP/UDP: 443 | |
| RIESGO | Un atacante sin privilegios puede abusar de la funcionalidad HTTP TRACE/TRACK para obtener acceso a información confidencial en encabezados al realizar solicitudes HTTP. | |
| DESCRIPCIÓN | El servidor web remoto admite los métodos TRACE y/o TRACK. TRACE y TRACK son métodos HTTP que se utilizan para depurar conexiones de servidor web. | |
| PROPUESTA DE REMEDIACIÓN | Se recomienda deshabilitar estos métodos HTTP. | |
| REFERENCIAS EXTERNAS | https://www.cgisecurity.com/whitehat-mirror/WH-WhitePaper\_XST\_ebook.pdf  http://www.apacheweek.com/issues/03-01-24  https://download.oracle.com/sunalerts/1000718.1.html | |

La vulnerabilidad se presenta en la siguiente ruta:

* https://cursosenlinea.sre.gob.mx/

A continuación, se presenta la evidencia de la vulnerabilidad detectada.



En la imagen se muestra como el servidor responde a este tipo de solicitudes.

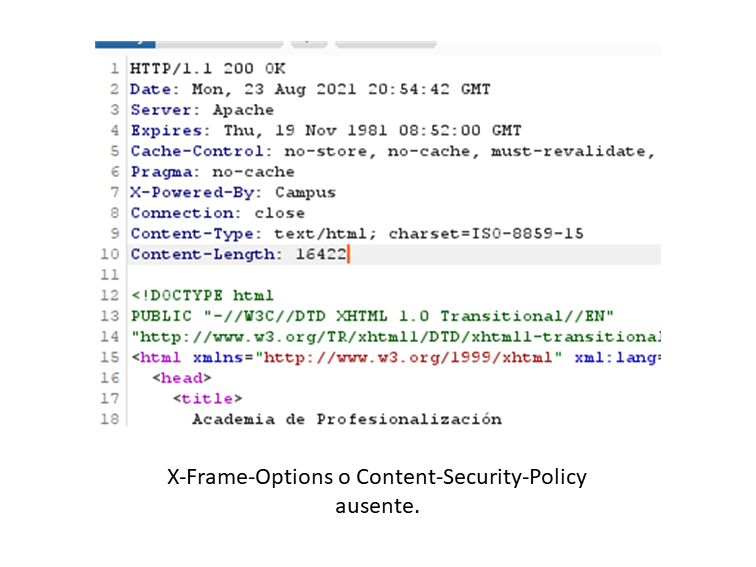
## Aplicación web potencialmente vulnerable al secuestro de clics

| **CWE-693** | APLICACIÓN WEB POTENCIALMENTE VULNERABLE AL SECUESTRO DE CLICS | **-** |
| --- | --- | --- |
| VALORACIÓNCVSS FINAL:  AV:A/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:N | | |
| NÚMERO DE OCURRENCIAS  1 | | |
| CLASIFICACIÓN  - | | |
| Dirección IP:  74.208.218.19 | Puerto TCP/UDP: 443 | |
| RIESGO | Un atacante puede engañar a un usuario para que haga clic en un área de la página vulnerable que es diferente de lo que el usuario percibe que es la página. Esto puede dar lugar a que un usuario realice transacciones fraudulentas o malintencionadas. | |
| DESCRIPCIÓN | El servidor web remoto no establece un encabezado de respuesta X-Frame-Options ni un encabezado de respuesta Content-Security-Policy ‘frame-ancestors’ en todas las respuestas de contenido. | |
| PROPUESTA DE REMEDIACIÓN | Se recomienda devolver el encabezado HTTP X-Frame-Options o Content-Security-Policy (con la directiva ‘frame-ancestors’) con la respuesta de la página para evitar que el contenido de la página sea incrustado por otro sitio. | |
| REFERENCIAS EXTERNAS | https://cwe.mitre.org/data/definitions/287.html  https://www.security-database.com/cwe.php?name=CWE-287 | |

La vulnerabilidad se presenta en la siguiente ruta:

* https://cursosenlinea.sre.gob.mx/
* https://cursosenlinea.sre.gob.mx/index.php
* https://cursosenlinea.sre.gob.mx/main/auth/lostPassword.php

A continuación, se presenta la evidencia de la vulnerabilidad detectada.



En la imagen se muestra la ausencia de estas cabeceras, aunque no pareciera que vulneran directamente la aplicación, permiten que la página se inserte en otros sitios diseñados que pueden ser maliciosos.

# Descripción de la criticidad

Para la evaluación de la criticidad, se emplea la siguiente categorización:

|  |  |
| --- | --- |
| **Colorimetría** | **Criticidad** |
|  | **CRÍTICA:** Estas vulnerabilidades son reportadas al momento de identificarlas en los equipos que, de acuerdo con el resultado de las pruebas de penetración, requieren de una acción inmediata, ya que pueden ser explotadas en el uso de la lógica de negocio del aplicativo, así también pueden ser explotadas fácilmente por un atacante poniendo en riesgo latente los activos de la institución. |
|  | **ALTA:** Equipos que, de acuerdo con el resultado de las pruebas de penetración, requieren de atención o una acción inmediata. Estas vulnerabilidades pueden ser explotadas fácilmente por un atacante poniendo en riesgo los activos de la empresa. |
|  | **MEDIA:** Estas vulnerabilidades son consecuencia de una configuración predeterminada o falta de aseguramiento en los activos. Su presencia no pone en riesgo inminente la integridad o confidencialidad de la información, sin embargo, es necesario mitigarlas. |
|  | **BAJA:** Equipos que tienen habilitados algunos puertos o servicios comunes de acuerdo al sistema operativo y que son necesarios, pero susceptibles de sufrir alguna vulnerabilidad. |
|  | **INFORMATIVA:** Notificaciones de sistema que no representan una vulnerabilidad, son de carácter informativo de algún puerto o servicio descubierto durante la aplicación de la prueba. |

# Resumen técnico de hallazgos

* Un atacante podría obtener de credenciales válidas para acceder al aplicativo.
* Un atacante podría realizar ataques de degradación, ataques de tipo "Man in the middle" que eliminan SSL y debilita las protecciones de secuestro de cookies.
* Un atacante podría explotar las vulnerabilidades conocidas del componente utilizado en la aplicación.
* Un atacante sin privilegios puede abusar de la funcionalidad HTTP TRACE/TRACK para obtener acceso a información confidencial en encabezados al realizar solicitudes HTTP.
* Un atacante puede engañar a un usuario para que haga clic en un área de la página vulnerable que es diferente de lo que el usuario percibe que es la página. Esto puede dar lugar a que un usuario realice transacciones fraudulentas o malintencionadas.

# Recomendaciones

* Se recomienda habilitar mecanismos de protección ante cierto número de intentos fallidos, por ejemplo 5 intentos consecutivos. Considere un periodo de espera para que los usuarios puedan volver a autenticarse después de los intentos fallidos.
* Se recomienda configurar el servidor web remoto para utilizar HSTS.
* Instalar los parches de seguridad correspondientes o actualizar a la última versión del componente.
* Se recomienda deshabilitar estos métodos HTTP.
* Se recomienda devolver el encabezado HTTP X-Frame-Options o Content-Security-Policy (con la directiva 'frame-ancestors') con la respuesta de la página para evitar que el contenido de la página sea incrustado por otro sitio.

# Firmas y fechas de elaboración, revisión, recepción y aprobación

**Por parte del proveedor:**

|  |  |
| --- | --- |
| Fecha: | 24/08/2021 |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Elabora** |  | **Revisa** |  | **Aprueba** |
| Osvaldo Hernández Morales  Operador de Controles Tecnológicos TIC Defense S.A. DE C.V. |  | Lázaro Santiago Cruz  Administrador del Centro de Operaciones de Seguridad (CiberSOC) TIC Defense S.A. DE C.V. |  | Reyes Abraham Orozco Macías  Líder del Proyecto  TIC Defense S.A. DE C.V. |

**Por parte de la secretaría:**

|  |  |
| --- | --- |
| Fecha: | 24/08/2021 |

|  |  |  |
| --- | --- | --- |
| **Recibe** |  | **Vo. Bo.** |
| Lic. Jessica Magalli Torres Mejía  Subdirectora de Seguridad Tecnológica  SRE |  | Ing. Juan Víctor Reyna Villanueva  Director de Seguridad Tecnológica  SRE |